RSAC 2025 Conference

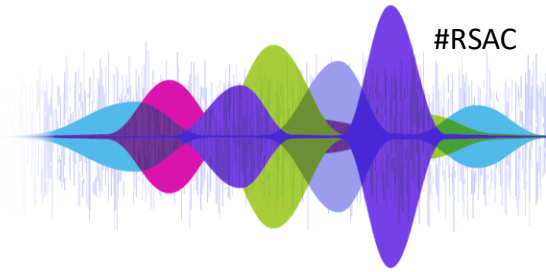
Many Voices. One Community.

SESSION ID: LAB1-T01

Cloud 9 Security: Unlocking Cloud-Native Security Posture Management Powers

Michael Ratemo

Principal Security Consultant
Cyber Security Simplified
https://www.linkedin.com/in/michael-ratemo/



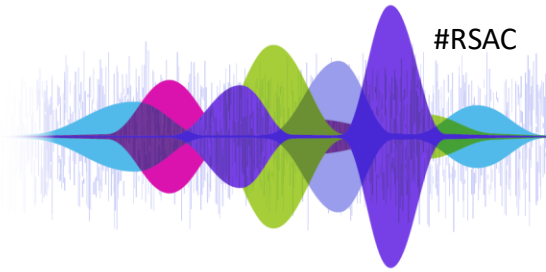
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Agenda



- 1. Welcome and Introduction
- 2. Challenges of Securing the Cloud
- 3. Overview of Cloud Security Posture Management (CSPM) Solutions
- 4. Review lab scenarios leveraging Amazon Web services (AWS) Security Hub, and Microsoft Defender for Cloud CSPM solutions
- 5. Attendees perform two separate labs including break out sessions
- 6. Wrap-up
  - Share key takeaways, highlighting common themes, and Best Practices for securing Cloud environments

Challenges of Securing the Cloud

- Misconfigurations
- Cloud Complexity / Dynamic Environments
- Threat Landscape Evolution
- Visibility and Monitoring
- Lack of Expertise

82% of data breaches involved data stored in cloud environments

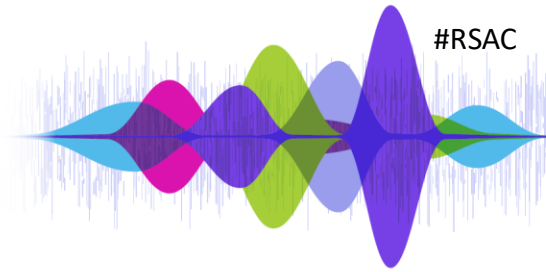
Cloud Security Posture Management Solutions

Benefits of CSPM Solutions

Centralized Visibility

Automated Remediation

Compliance Management



Cloud-Native vs Third Party CSPM Solutions

Cloud-Native CSPM Solutions	Third Party CSPM Solutions
✓ AWS Security Hub	✓ Prisma Cloud by Palo Alto Networks
✓ Microsoft Defender for Cloud	✓ CrowdStrike Falcon Cloud Security
✓ Google Cloud Security Command Center	✓ Wiz

Cloud-Native Cloud Security Posture Management

AWS Security Hub

Microsoft Defender for Cloud

Google Cloud Security Command Centre

RSAC 2025 Conference

Cloud-Native Security Posture Management

Let us Dive into the Labs Part 1

Cyber Security Simplified

We speak security in the language you understand

Many Voices.
One Community.

Cloud Security Posture Management Lab 1 Instructions

- You have 15 minutes in total to complete the paper exercise – Common Cloud Misconfigurations
- Follow the instructions in your lab handouts
- If you have any questions or need help, please let us know
- Relax and have fun
- We will breakout at the end or the lab to review and share findings

RSAC 2025 Conference

Cloud-Native Security Posture Management

Let us Dive into the Labs Part 2

Cyber Security Simplified

We speak security in the language you understand

Many Voices.
One Community.

Cloud Security Posture Management Lab 1 Instructions

- You have 30 minutes in total to complete these labs across AWS Security Hub CSPM Lab.
- Follow the instructions in your lab handouts
- If you have any questions or need help, please let us know
- Relax and have fun
- We will breakout at the end or the lab to review and share findings

RSAC 2025 Conference

Cloud-Native Security Posture Management

Let us Dive into the Labs Part 3

Cyber Security Simplified

We speak security in the language you understand

Many Voices.
One Community.

Cloud Security Posture Management Lab 3 Instructions

- You have 30 minutes in total to complete the Microsoft Defender for Cloud CSPM lab
- Follow the instructions in your lab handouts
- If you have any questions or need help, please let us know
- Relax and have fun
- We will breakout at the end or the lab to review and share findings

RSAC 2025 Conference

Bringing it all Together

Wrap-up

Cyber Security Simplified

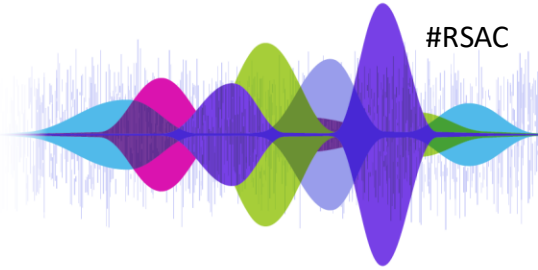
We speak security in the language you understand

Many Voices.
One Community.

Best Practices for securing Cloud environments

1. Implement Cloud Governance
2. Adhere to the Shared Responsibility Model
3. Automation with Infrastructure as Code (IaC) templates
4. Leverage Cloud Service Provider Solutions
5. Utilize Configuration Management tools
6. Implement Continuous Monitoring and Alerts
7. Employ robust Technical Controls (MFA, Encryption, Principle of Least Privilege, Logging & Monitoring)
8. Education and Training

Apply What You Have Learned Today



- **Next week you should:**
  - Perform a CSPM scan to identify misconfigurations and compliance gaps.
  - Document initial findings for internal discussion.
- **In the first three months following this presentation you should:**
  - Implement automated security policies and alerts within CSPM to proactively detect and mitigate risks.
- **Within six months you should:**
  - Conduct a comprehensive CSPM-driven assessment to measure improvements and identify remaining gaps.
  - Enhance cloud security posture by refining compliance reporting, and integrating CSPM with broader security and governance frameworks.

Additional Resources

- **Cloud Security Posture Management (CSPM) courses in AWS, Azure, and Google Cloud on LinkedIn Learning by Michael Ratemo**
- https://www.linkedin.com/learning/amazon-web-services-aws-cloud-security-posture-management-cspm-24560222/
- https://www.linkedin.com/learning/microsoft-azure-cloud-security-posture-management-cspm/
- https://www.linkedin.com/learning/google-cloud-cloud-security-posture-management-cspm/

Additional Resources

- **Cloud Security and Audit Fundamentals course in AWS, Azure and Google Cloud on LinkedIn Learning by Michael Ratemo**
- https://www.linkedin.com/learning/cloud-security-and-audit-fundamentals-aws-microsoft-azure-and-google-cloud

- **Cloud Auditing Best Practices Book: Perform Security and IT Audits across AWS, Azure, and GCP by Building Effective Cloud Auditing Plans by** *Shinesa Cambric* **and** *Michael Ratemo*

RSAC 2025 Conference

Many Voices.
One Community.

THANK YOU !

Further Discussion/Information:

info@cybersecuritysimplified.com

https://www.cybersecuritysimplified.com

Cyber Security Simplified

We speak security in the language you understand